United Nations A/CN.9/483

General Assembly

Distr.: General
6 October 2000

Original: English

United Nations Commission on International Trade Law
Thirty-fourth session
Vienna, 25 June-13 July 2001

Report of the Working Group on Electronic Commerce on the work of its thirty-seventh session (Vienna, 18-29 September 2000)

Contents

		Paragraphs	*Page*
Introduction		1-20	2
I.	Deliberations and decisions	21-23	5
II.	Draft articles on electronic signatures	24-144	6
A.	General remarks	24	6
B.	Consideration of draft articles	25-133	6
Article 12.	Recognition of foreign certificates and electronic signatures	25-58	6
Article 2.	Definitions	59-109	16
Article 5.	Variation by agreement	110-113	27
Article 9.	Conduct of the certification service provider	114-127	28
Article 10.	Trustworthiness	128-133	32
C.	Form of the instrument	134-138	33
D.	Relationship with the UNCITRAL Model Law on Electronic Commerce	139-142	34
E.	Report of the drafting group	143-144	34
III.	Draft guide to enactment	145-152	35
A.	General remarks	145-147	35
B.	Specific remarks	148-152	36
Annex	Draft UNCITRAL Model Law on Electronic Signatures		39

V.00-57852

Introduction

1. The Commission, at its twenty-ninth session (1996), decided to place the issues of digital signatures and certification authorities on its agenda. The Working Group on Electronic Commerce was requested to examine the desirability and feasibility of preparing uniform rules on those topics. It was agreed that the uniform rules to be prepared should deal with such issues as: the legal basis supporting certification processes, including emerging digital authentication and certification technology; the applicability of the certification process; the allocation of risk and liabilities of users, providers and third parties in the context of the use of certification techniques; the specific issues of certification through the use of registries; and incorporation by reference.[1]

2. At its thirtieth session (1997), the Commission had before it the report of the Working Group on the work of its thirty-first session (A/CN.9/437). The Working Group indicated to the Commission that it had reached consensus as to the importance of, and the need for, working towards harmonization of law in that area. While no firm decision as to the form and content of such work had been reached, the Working Group had come to the preliminary conclusion that it was feasible to undertake the preparation of draft uniform rules at least on issues of digital signatures and certification authorities, and possibly on related matters. The Working Group recalled that, alongside digital signatures and certification authorities, future work in the area of electronic commerce might also need to address: issues of technical alternatives to public-key cryptography; general issues of functions performed by third-party service providers; and electronic contracting (A/CN.9/437, paras. 156-157). The Commission endorsed the conclusions reached by the Working Group and entrusted the Working Group with the preparation of draft uniform rules on the legal issues of digital signatures and certification authorities (also referred to in this report as "the draft uniform rules" or "the uniform rules").

3. With respect to the exact scope and form of the uniform rules, the Commission generally agreed that no decision could be made at this early stage of the process. It was felt that, while the Working Group might appropriately focus its attention on the issues of digital signatures in view of the apparently predominant role played by public-key cryptography in the emerging electronic-commerce practice, the uniform rules should be consistent with the media-neutral approach taken in the UNCITRAL Model Law on Electronic Commerce (hereinafter referred to as "the Model Law"). Thus, the uniform rules should not discourage the use of other authentication techniques. Moreover, in dealing with public-key cryptography, the uniform rules might need to accommodate various levels of security and to recognize the various legal effects and levels of liability corresponding to the various types of services being provided in the context of digital signatures. With respect to certification authorities (a concept that was later replaced by that of "certification service provider" by the Working Group: see below, paras. 66 and 89), while the value of market-driven standards was recognized by the Commission, it was widely felt that the Working Group might appropriately envisage the establishment of a minimum set of standards to be met by certification authorities, particularly where cross-border certification was sought.[2]

4. The Working Group began the preparation of the uniform rules at its thirty-second session on the basis of a note prepared by the Secretariat (A/CN.9/WG.IV/WP.73).

5. At its thirty-first session (1998), the Commission had before it the report of the Working Group on the work of its thirty-second session (A/CN.9/446). It was noted that the Working Group, throughout its thirty-first and thirty-second sessions, had experienced manifest difficulties in reaching a common understanding of the new legal issues that arose from the increased use of digital and other electronic signatures. It was also noted that a

consensus was still to be found as to how those issues might be addressed in an internationally acceptable legal framework. However, it was generally felt by the Commission that the progress realized so far indicated that the draft uniform rules on electronic signatures were progressively being shaped into a workable structure.

6. The Commission reaffirmed the decision made at its thirtieth session as to the feasibility of preparing such uniform rules and expressed its confidence that more progress could be accomplished by the Working Group at its thirty-third session on the basis of the revised draft prepared by the Secretariat (A/CN.9/WG.IV/WP.76). In the context of that discussion, the Commission noted with satisfaction that the Working Group had become generally recognized as a particularly important international forum for the exchange of views regarding the legal issues of electronic commerce and for the preparation of solutions to those issues.[3]

7. The Working Group continued revision of the uniform rules at its thirty-third (1998) and thirty-fourth (1999) sessions on the basis of notes prepared by the Secretariat (A/CN.9/WG.IV/WP.76 and A/CN.9/WG.IV/WP.79 and 80).

8. At its thirty-second session (1999), the Commission had before it the report of the Working Group on the work of those two sessions (A/CN.9/454 and 457). The Commission expressed its appreciation for the efforts accomplished by the Working Group in its preparation of draft uniform rules on electronic signatures. While it was generally agreed that significant progress had been made at those sessions in the understanding of the legal issues of electronic signatures, it was also felt that the Working Group had been faced with difficulties in building a consensus as to the legislative policy on which the uniform rules should be based.

9. A view was expressed that the approach currently taken by the Working Group did not sufficiently reflect the business need for flexibility in the use of electronic signatures and other authentication techniques. As currently envisaged by the Working Group, the uniform rules placed excessive emphasis on digital signature techniques and, within the sphere of digital signatures, on a specific application involving third-party certification. Accordingly, it was suggested that work on electronic signatures by the Working Group should either be limited to the legal issues of cross-border certification or be postponed altogether until market practices were better established. A related view expressed was that, for the purposes of international trade, most of the legal issues arising from the use of electronic signatures had already been solved in the UNCITRAL Model Law on Electronic Commerce. While regulation dealing with certain uses of electronic signatures might be needed outside the scope of commercial law, the Working Group should not become involved in any such regulatory activity.

10. The widely prevailing view was that the Working Group should pursue its task on the basis of its original mandate (see above, paras. 2 and 3). With respect to the need for uniform rules on electronic signatures, it was explained that, in many countries, guidance from UNCITRAL was expected by governmental and legislative authorities that were in the process of preparing legislation on electronic signature issues, including the establishment of public key infrastructures (also referred to in this report as "PKI") or other projects on closely related matters (see A/CN.9/457, para. 16). As to the decision made by the Working Group to focus on PKI issues and PKI terminology, it was recalled that the interplay of relationships between three distinct types of parties (i.e., key holders, certification authorities and relying parties) corresponded to one possible PKI model, but that other models were conceivable, e.g., where no independent certification authority was involved. One of the main benefits to be drawn from focusing on PKI issues was to facilitate the structuring of the uniform rules by reference to three functions (or roles) with respect to key pairs, namely, the key issuer (or subscriber) function, the certification

function and the relying function. It was generally agreed that those three functions were common to all PKI models. It was also agreed that those three functions should be dealt with irrespective of whether they were in fact served by three separate entities or whether two of those functions were served by the same person (e.g., where the certification authority was also a relying party). In addition, it was widely felt that focusing on the functions typical of PKI and not on any specific model might make it easier to develop a fully media-neutral rule at a later stage (ibid., para. 68).

11. After discussion, the Commission reaffirmed its earlier decisions as to the feasibility of preparing such uniform rules (see above, paras. 2 and 6) and expressed its confidence that more progress could be accomplished by the Working Group at its forthcoming sessions.[4]

12. The Working Group continued revision of the uniform rules at its thirty-fifth (September 1999) and thirty-sixth (February 2000) sessions on the basis of notes prepared by the Secretariat (A/CN.9/WG.IV/WP.82 and WP.84). The reports of those two sessions are contained in documents A/CN.9/465 and 467.

13. At its thirty-third session (New York, 12 June - 7 July 2000), the Commission noted that the Working Group, at its thirty-sixth session, had adopted the text of draft articles 1 and 3 to 11 of the uniform rules. The view was expressed that some issues remained to be clarified as a result of the deletion from the draft uniform rules of the notion of "enhanced electronic signature". It was stated that, depending on the decision to be made by the Working Group with respect to draft articles 2 (Definitions) and 12 (Recognition of foreign certificates and foreign electronic signatures), the remainder of the draft provisions might need to be revisited to avoid creating a situation where the standard set forth by the uniform rules would apply equally to electronic signatures that ensured a high level of security and to low-value certificates that might be used in the context of electronic communications that were not intended to carry significant legal effect.

14. After discussion, the Commission expressed its appreciation for the efforts accomplished by the Working Group and the progress achieved in the preparation of the draft uniform rules. The Working Group was urged to complete its work with respect to the draft uniform rules at its thirty-seventh session, and to review the draft guide to enactment to be prepared by the Secretariat.[5]

15. The Working Group on Electronic Commerce, which was composed of all the States members of the Commission, held its thirty-seventh session at Vienna from 18 to 29 September 2000. The session was attended by representatives of the following States members of the Working Group: Argentina, Australia, Austria, Brazil, Cameroon, China, Colombia, Egypt, France, Germany, Honduras, Hungary, India, Iran (Islamic Republic of), Italy, Japan, Mexico, Nigeria, Romania, Russian Federation, Singapore, Spain, Thailand, United Kingdom of Great Britain and Northern Ireland, and United States of America.

16. The session was attended by observers from the following States: Belgium, Canada, Costa Rica, Cuba, Czech Republic, Ecuador, Guatemala, Indonesia, Ireland, Jordan, Lebanon, Malaysia, Malta, Morocco, Netherlands, New Zealand, Peru, Poland, Portugal, Republic of Korea, Saudi Arabia, Slovakia, Sweden, Switzerland, Tunisia, Turkey, Ukraine, Uruguay and Yemen.

17. The session was also attended by observers from the following international organizations: *(a) United Nations system:* Economic Commission for Europe (UN/ECE), United Nations Conference on Trade and Development (UNCTAD), World Bank; *(b) Intergovernmental organizations:* African Development Bank (ADB), Commonwealth Secretariat, European Commission, European Space Agency (ESA),

Organisation for Economic Co-operation and Development (OECD); *(c) International organizations invited by the Commission:* Cairo Regional Centre for International Commercial Arbitration, European Law Students' Association (ELSA), International Association of Ports and Harbors (IAPH), International Bar Association (IBA), International Chamber of Commerce (ICC) and *Union internationale du notariat latin* (UINL).

18. The Working Group elected the following officers:

Chairman: Mr. Jacques GAUTHIER (Canada, elected in his personal capacity);

Rapporteur: Mr. Pinai NANAKORN (Thailand).

19. The Working Group had before it the following documents: provisional agenda (A/CN.9/WG.IV/WP.85); note by the Secretariat containing draft uniform rules on electronic signatures (A/CN.9/WG.IV/WP.84); and two notes by the Secretariat containing the draft guide to enactment of the uniform rules (A/CN.9/WG.IV/WP.86 and A/CN.9/WG.IV/WP.86/Add.1).

20. The Working Group adopted the following agenda:

1. Election of officers.
2. Adoption of the agenda.
3. Legal aspects of electronic commerce:
   Draft uniform rules on electronic signatures
   Draft guide to enactment of the uniform rules on electronic signatures
   Possible future work in the field of electronic commerce
4. Other business.
5. Adoption of the report.

I. Deliberations and decisions

21. The Working Group discussed the issues of electronic signatures on the basis of the note prepared by the Secretariat (A/CN.9/WG.IV/WP.84) and the draft articles adopted by the Working Group at its thirty-sixth session (A/CN.9/467, Annex). The deliberations and conclusions of the Working Group with respect to those issues are reflected in section II below.

22. After discussing draft articles 2 and 12 (numbered 13 in document A/CN.9/WG.IV/WP.84), and considering consequential changes in other draft articles, the Working Group adopted the substance of the draft articles and referred them to a drafting group to ensure consistency between the provisions of the uniform rules. The Working Group subsequently reviewed and amended the provisions adopted by the drafting group. The final version of the draft provisions as adopted by the Working Group is contained in the annex to this report.

23. The Working Group discussed the draft guide to enactment of the uniform rules. The deliberations and conclusions of the Working Group in that respect are reflected in section III below. The Secretariat was requested to prepare a revised version of the draft guide reflecting the decisions made by the Working Group, based on the various views,

suggestions and concerns that had been expressed at the current session. Due to lack of time, the Working Group did not complete its deliberations regarding the draft guide to enactment. It was agreed that some time should be set aside by the Working Group at its thirty-eighth session for completion of that agenda item. It was noted that the draft uniform rules (now in the form of a draft UNCITRAL Model Law on Electronic Signatures), together with the draft guide to enactment, would be submitted to the Commission for review and adoption at its thirty-fourth session, to be held at Vienna from 25 June to 13 July 2001.

II. Draft articles on electronic signatures

A. General remarks

24. At the outset, the Working Group exchanged views on current developments in regulatory issues arising from electronic commerce, including adoption of the Model Law, electronic signatures and public key infrastructure (referred to here as "PKI") issues in the context of digital signatures. These reports, at the governmental level, confirmed that addressing electronic commerce legal issues was recognized as essential for the implementation of electronic commerce and the removal of barriers to trade. It was reported that a number of countries had introduced recently, or were about to introduce, legislation either adopting the Model Law or addressing related electronic commerce facilitation issues. A number of those legislative proposals also dealt with electronic (or in some cases, specifically digital) signature issues.

B. Consideration of draft articles

Article 12. Recognition of foreign certificates and electronic signatures

25. The text of draft article 12 (numbered 13 in document A/CN.9/WG.IV/WP.84) as considered by the Working Group was as follows:

"[(1) In determining whether, or the extent to which, a certificate [or an electronic signature] is legally effective, no regard shall be had to the place where the certificate [or the electronic signature] was issued, nor to the State in which the issuer had its place of business.]

"(2) Certificates issued by a foreign supplier of certification services are recognized as legally equivalent to certificates issued by suppliers of certification services operating under ... *[the law of the enacting State]* if the practices of the foreign suppliers of certification services provide a level of reliability at least equivalent to that required of suppliers of certification services under ... *[the law of the enacting State]*. [Such recognition may be made through a published determination of the State or through bilateral or multilateral agreement between or among the States concerned.]

"(3) Signatures complying with the laws of another State relating to electronic signatures are recognized as legally equivalent to signatures under ... *[the law of the enacting State]* if the laws of the other State require a level of reliability at least equivalent to that required for such signatures under ... *[the law of the enacting State]*. [Such recognition may be made by a published determination of the State or through bilateral or multilateral agreement with other States.]

"(4) In determining equivalence, regard shall be had, if appropriate, [to the factors in paragraph (2) of article 10] [to the following factors:

"(a) financial and human resources, including existence of assets within the jurisdiction;

"(b) trustworthiness of hardware and software systems;

"(c) procedures for processing of certificates and applications for certificates and retention of records;

"(d) availability of information to the [signers][subjects] identified in certificates and to potential relying parties;

"(e) regularity and extent of audit by an independent body;

"(f) the existence of a declaration by the State, an accreditation body or the certification authority regarding compliance with or existence of the foregoing;

"(g) susceptibility to the jurisdiction of courts of the enacting State; and

"(h) the degree of discrepancy between the law applicable to the conduct of the certification authority and the law of the enacting State].

"(5) Notwithstanding paragraphs (2) and (3), parties to commercial and other transactions may specify that a particular supplier of certification services, class of suppliers of certification services or class of certificates must be used in connection with messages or signatures submitted to them.

"(6) Where, notwithstanding paragraphs (2) and (3), parties agree, as between themselves, to the use of certain types of electronic signatures and certificates,[that agreement shall be recognized as sufficient for the purpose of cross-border recognition]. [In determining whether, or the extent to which, an electronic signature or certificate is legally effective, regard shall be had to any agreement between the parties to the transaction in which that signature or certificate is used.]"

Paragraph (1)

26. It was pointed out that, in connection with certificates, the qualification "foreign" clearly denoted a certificate issued by a certification authority operating outside the jurisdiction where the certificate was invoked. In contrast, the notion of a "foreign" signature, be it hand-written or in electronic form, was not equally clear since various criteria might be used to qualify a signature as "foreign" (such as the place where the signature was produced, the nationality of the parties, the place of operations of the certification authority). Therefore, the suggestion was made that the scope of paragraph (1) should be confined to the recognition of foreign certificates and that the words "or an electronic signature", which currently appeared within square brackets, should be deleted. While some support was expressed to that suggestion, the prevailing view was that paragraph (1) should cover both certificates and signatures and the square brackets around the words "or an electronic signature" should be removed. It was pointed out, in that connection, that electronic signatures were not always accompanied by a certificate and that electronic signature generated without an attached certificate should also benefit from the non-discrimination rule stated in paragraph (1).

27. The view was expressed that the phrase "no regard shall be had [...] to the place where the certificate or the electronic signature was issued" was excessively

categorical for the purposes of paragraph (1). The provision, it was suggested, might be more clearly expressed by using instead words such as "[d]etermination of whether, or the extent to which, a certificate or an electronic signature is legally effective shall not depend on the place where the certificate or the electronic signature was issued [...]". Another suggestion was to rephrase paragraph (1) along the following lines: "A certificate or an electronic signature shall not be denied effect only on the basis of the place it emanates from." In response to those suggestions, it was stated that the wording currently used adequately reflected the purpose of paragraph (1), as it made it clear that the place of origin, in and of itself, should in no way be a factor determining whether and to what extent foreign certificates or electronic signatures were legally effective. After consideration of the different views expressed, the Working Group decided to retain the current text of paragraph (1), subject to removing all square brackets, and referred it to the drafting group.

Paragraph (2)

28. As a general comment, it was stated by a number of delegations that paragraph (1) already contained the fundamental principles to be followed in respect of the recognition of foreign certificates and electronic signatures, so that paragraph (2) and the remainder of draft article 13 were not necessary. Furthermore, it was said that paragraph (2) might have unintended discriminatory effects, since the references in italics to legal requirements in the enacting State appeared to link the recognition of foreign certificates or electronic signatures to the existence of a governmental licensing regime for certification authorities (the concept of "certification authority" was later replaced by that of "certification service provider" by the Working Group: see below, paras. 66 and 89). Therefore, it was proposed that paragraphs (2) through (6) should be replaced with the following provisions:

> "(2) To the extent that a State does condition the recognition of a certificate [or an electronic signature], any condition should be satisfied through accreditation by a private sector voluntary accreditation mechanism.
>
> "(3) Where, notwithstanding paragraph (2), parties agree, as between themselves, to the use of certain types of electronic signatures and certificates, that agreement shall be recognized as sufficient for the purpose of cross-border recognition."

29. While some support was expressed in favour of the proposal, the prevailing view was that, although its wording might require some improvement, paragraph (2) contained important provisions, which needed to be retained in the text of the uniform rules. It was noted that the Working Group had acknowledged early on that domestic jurisdictions might use various approaches for dealing with certification functions, ranging from mandatory licensing regimes under governmental control to private sector voluntary accreditation schemes. It was not the intention of draft article 12 to impose or exclude any of such approaches but rather to set forth criteria for the recognition of foreign certificates and electronic signatures, which would be valid and pertinent regardless of the nature of the certification scheme obtaining in the jurisdiction from which the certificate or signature emanated. Nevertheless, the Working Group acknowledged that the phrase inviting the enacting State to indicate the law under which suppliers of certifications services operated might be given an undesirably narrow interpretation, and agreed that alternative wording, such as "in this State" or "in this jurisdiction" should be used instead.

30. Turning its attention to the current text of paragraph (2), the Working Group heard expressions of concern that the purpose of the provision was not entirely clear. Three interpretations, it was said, could be given to paragraph (2), namely: (a) that foreign suppliers of certification services should be given equal opportunity to have

their services recognized through registration under the laws of the enacting State; (b) that certificates issued by foreign suppliers of certification services should, under the circumstances provided in paragraph (2) have the same legal effect as certificates issued by recognized certification authorities in the enacting State; or (c) that foreign suppliers of certification services should benefit from fast-track recognition in the enacting State if they met the requirements set forth in paragraph (2). If the first interpretation was correct, paragraph (2) was not needed, since it would merely restate the non-discrimination principle of paragraph (1). If the second interpretation was correct, paragraph (2) might place a foreign supplier of certification services that was not subject to mandatory licensing in its country of origin in equal standing with licensed domestic certification authorities, thus resulting in undesirable reverse discrimination against suppliers of certification services that needed to obtain a license in the enacting State. If the third interpretation was correct, it should be spelled out more clearly.

31. In response to those interpretations and concerns, it was pointed out that the purpose of paragraph (2) was not to place foreign suppliers of certification services in a better position than domestic ones, but to provide criteria for the cross-border recognition of certificates without which suppliers of certification services would face the unreasonable burden of having to obtain licenses in multiple jurisdictions. For that purpose, paragraph (2) established a threshold for technical equivalence of foreign certificates based on testing their reliability against the reliability requirements established by the enacting State pursuant to the uniform rules. Whether, for the licensing of domestic suppliers of certification services, an enacting State chose to establish additional criteria above and beyond those set out in paragraph (3), or whether the country of origin imposed criteria higher than those, was a policy decision outside the scope of the uniform rules.

32. The view was expressed that the requirement that the level of reliability of the practices of foreign suppliers of certification services should be "at least" equivalent to that required in the enacting State was excessively restrictive and inappropriate in an international context. It was important to acknowledge that there might be significant variance between the requirements of individual jurisdictions. Therefore, it would be more appropriate to require that the level of reliability of the practices of suppliers of certification services should be "comparable", rather than "at least equivalent", to that of domestic ones. The Working Group considered at length the appropriate threshold for the recognition of foreign certificates. There was general sympathy for the concerns that had been expressed regarding the difficulty of establishing equivalence of certificates in an international context. It was felt, however, that the notion of a "comparable" level of reliability in the practices of suppliers of certification services did not afford the degree of legal certainty that might be needed to promote cross-border use of certificates. After consideration of various alternatives, the Working Group decided that paragraph (2) should refer to a level of reliability "substantially" equivalent to that obtaining in the enacting State. The Working Group noted, in that connection, that the requirement of equivalence, as used in paragraph (2), did not mean that the level of reliability of the foreign certificate should be exactly identical with that of domestic ones.

33. It was pointed out that paragraph (2) seemed to imply that there would be a single set of requirements for all types of certificates. In practice, however, suppliers of certification services issued certificates with various levels of reliability, according to the purposes for which the certificates were intended to be used by their customers. Depending on their respective level of reliability, not all certificates were worth producing legal effects, either domestically or abroad. Therefore, it was suggested that paragraph (2) should be reformulated so as to reflect the idea that the equivalence to be established was as between certificates of the same type. The Working Group was

mindful of the need to take into account the various levels of certificate and the type of recognition or legal effect each might deserve depending on their respective level of reliability. However, the prevailing view was that the proposed reformulation of paragraph (2) was problematic because of the difficulty of establishing the correspondence between certificates of different types issued by different suppliers of certification services in different jurisdictions. For that reason, the uniform rules had been drafted so as to contemplate a possible hierarchy of different types of certificate. Furthermore, it was said that the issue of different types of certificates was a matter for the practical application of the uniform rules and that appropriate reference in the draft guide to enactment might suffice. In practice, a court or arbitral tribunal called upon to decide on the legal effect of a foreign certificate would normally consider each certificate on its own merit and try to equate it with the closest corresponding level in the enacting State.

34. Another comment was that, although the essence of paragraph (2) was satisfactory, its purpose would be better served if paragraph (2) would clearly provide for the legal effectiveness, rather than the recognition, of foreign certificates issued in accordance with practices found to be substantially equivalent to those required in the enacting State. The notion of recognition, which was known in other areas of the law (for example in connection with recognition and enforcement of foreign arbitral awards), was said to imply that a special procedure might be required in each instance, before a foreign certificate could produce legal effects in the enacting State. If paragraph (2) was to have any practical significance beyond what was already contained in paragraph (1), the provision should be reformulated so as to affirm the legal effectiveness of foreign certificates and the conditions therefor.

35. While there was general support for recasting paragraph (2) to include the notion of legal effectiveness, the views differed as to whether the applicable standard should be dependent upon the reliability of the practices followed by the foreign supplier of certification services or whether such standard should be based on the level of reliability offered by the foreign certificate itself. The prevailing view that emerged in the course of the deliberations was that the standard to be used in paragraph (2) should be the level of reliability offered by the foreign certificate itself, when compared with the level of reliability offered by certificates issued by domestic suppliers of certification services. Focusing on the certificate, rather than the practices followed by the supplier of certification services, also made it easier to solve other problems raised by the current wording of paragraph (2). Indeed, the new wording of paragraph (2) made it more flexible and apt to take into account the various types of certificates and the varying level of reliability they provided, without having to refer in the text to different types of certificate.

36. The Working Group concluded its consideration of paragraph (2) by requesting the drafting group to reformulate the provision to the effect that a certificate issued by a foreign supplier of certification services should have the same legal effect as a certificate issued by a domestic supplier of certification services when such certificate afforded a substantially equivalent level of reliability. It was understood that the use of the words "a certificate", rather than "certificates", made it clear that the reliability test was to be applied in respect of each certificate, rather than to categories of certificates, or to all certificates of a particular supplier of certification services.

Paragraph (3)

37. As a general comment, it was said that paragraph (3) appeared to contemplate criteria whereby the enacting State would validate electronic signatures produced abroad. If that was the case, paragraph (3) seemed to introduce, in respect of electronic signatures, a situation without precedent in the context of paper-based

transactions. Indeed, the validity of hand-written signatures was determined, as appropriate, by the law governing the transaction in question or by the law governing questions related to the legal capacity of the signatory. To the extent that paragraph (3) set forth an independent parameter for establishing the legal effect of an electronic signature, the provision interfered with well-established rules of private international law. The Working Group, therefore, was urged to consider deleting the provision.

38. The Working Group was of the view, however, that paragraph (3) did not affect the functioning of the rules of private international law relevant to the validity of a signature, since it was concerned exclusively with standards for the cross-border recognition of the reliability of the method used to identify the signatory of any given electronic message. Nevertheless, it was generally felt that, for purposes of clarity, and with a view to aligning paragraphs (2) and (3), the references to the laws of States other than the enacting State should be deleted from paragraph (3).

39. In that connection, the view was expressed that a provision recognizing some legal effect in the enacting State to compliance with the laws of a foreign country was useful and, subject to clarifying the doubts that had been expressed earlier, the provision should be retained. It was said that what mattered for paragraph (3) was to establish a cross-border reliability test of the methods used for producing electronic signatures. The current formulation of paragraph (3) had the practical advantage of obviating the need for a reliability test in respect of specific signatures, when the enacting State was satisfied that the law of the jurisdiction from which the signature originated provided an adequate standard of reliability for electronic signatures. In response it was pointed out that the practical advantage that had been identified would still exist despite the deletion of the reference to the laws of the foreign State. In the context of that discussion, it was pointed out that electronic signatures were defined in draft article 2 as methods of identification and therefore the reliability test contemplated in paragraph (3) pertained to such method, rather than to the signature itself.

40. The view was expressed that, since both paragraphs (2) and (3) implemented the non-discrimination rule stated in paragraph (1) they could be usefully combined in a single provision. The prevailing view, however, was that, paragraphs (2) and (3) had a function of their own, which was distinct from paragraph (1). Paragraph (1) was a rule of non-discrimination formulated in negative terms, whereas paragraphs (2) and (3) developed that general rule in more concrete terms by positively affirming that foreign certificates and electronic signatures should be given legal effect when substantially equivalent to domestic ones in terms of their reliability. While the logical link between the three paragraphs could be made clearer (for example, by adding words such as "consequently" at the end of paragraph (1) and re-arranging paragraphs (2) and (3) as its subparagraphs), the substance of those two paragraphs should be retained. Furthermore, as different factors might need to be taken into account for the cross border-recognition of certificates and electronic signatures, each provision should be kept separate.

41. After discussion, the Working Group decided that the text of paragraph (3) should be brought in line with the structure of paragraph (2) and redrafted along the lines of "Electronic signatures issued in a foreign State shall produce the same legal effects as electronic signatures issued in ... *[the enacting State]*, provided that they offer a substantially equivalent level of reliability". The matter was referred to the drafting group.

42. As to the words in square brackets at the end of both paragraphs (2) and (3), it was generally agreed that the reference to the legal techniques through which advance recognition of the reliability of foreign certificates and signatures might be made by

an enacting State (i.e. a unilateral declaration or a treaty) should be not be part of the uniform rules. Instead, it should be discussed in the draft guide to enactment.

Paragraph (4)

43. The Working Group held an extensive discussion on the relevance of the criteria set forth in paragraph (4) for the purpose of cross-border recognition of foreign certificates and signatures, and the need for retaining such a provision in view of the amendments that had been agreed to in paragraphs (2) and (3). In that connection, strong support was expressed both for deleting paragraph (4) as well as for retaining it, possibly in a modified form. The view was also reiterated that paragraphs (2) and (3) should be deleted.

44. In favour of deleting paragraph (4) it was stated that, to the extent that the criteria listed therein were not identical with those listed in the relevant parts of draft articles 6, 9 and 10, paragraph (4) was inconsistent with the view taken by the Working Group at its thirty-fifth session, in 1999, that criteria set forth with respect to signatures or certificates should apply equally to foreign and domestic signatures or certificates (A/CN.9/465, para. 35). If, in turn, paragraph (4) were merely to reproduce criteria set forth earlier in the uniform rules, the provision would in practice be superfluous. Moreover, the criteria set forth in paragraph (4) were not entirely relevant for certificates or electronic signatures, since they included criteria contained in draft articles 9 and 10 that had been specifically conceived for the purpose of assessing the trustworthiness of suppliers of certification services. Another argument for the deletion of paragraph (4) was that the list was perceived as limiting party autonomy and impinging upon the freedom of judges and arbitrators to examine, in concrete cases, the reliability of certificates and signatures. Yet another reason for deleting paragraph (4) was that the listing of specific criteria for determining equivalence was inconsistent with the spirit of paragraphs (2) and (3), as newly amended by the Working Group. Indeed, paragraphs (2) and (3) envisaged a test of the substantial equivalence of foreign certificates and signatures, as compared to domestic ones. Such a test logically entailed a comparison of the respective standards of reliability obtaining in the jurisdictions concerned and not the referral to an independent set of criteria.

45. In favour of retaining paragraph (4) it was stated that although the list contained therein might not be entirely pertinent and might need to be revised, such a provision offered useful guidance for assessing the equivalence of certificates and signatures. Merely mentioning the relevant criteria in the draft guide to enactment, as had been suggested, would not achieve the intended result, since the draft guide was addressed to legislators and was not the type of document to which domestic courts would usually refer. A set of standards for assessing the equivalence of foreign certificates was needed, since that exercise was intrinsically different from the assessment of the trustworthiness of a supplier of certification services under draft articles 9 and 10. If the concern was that the criteria listed in paragraph (4) were not entirely pertinent to cross-border recognition of certificates and electronic signatures, reformulating the list would be a better solution than simply deleting it. For that purpose, the following alternative wording was proposed for paragraph (4):

"In determining whether a certificate offers a substantially equivalent level of reliability for the purpose of paragraph (2) regard shall be had to:

"1. the following aspects of the operational procedures of the foreign supplier of certification services:

"(a) the trustworthiness of hardware and software systems and the method of its

utilization;

"(b) procedures for:

"(i) the making of applications for certificates;

"(ii) the processing of certificate applications;

"(iii) the processing of certificates;

"(iv) the procedures for a signatory to give notice that a signature device has been compromised;

"(v) the procedures utilized for the operation of a timely revocation service.

"(c) the regularity and extent of any audit by an independent third party;

"2. the existence of a declaration by a State or an accreditation body in respect of all or any of the matters listed in para. (1)(b) above;

"3. recognized international standards met by the foreign supplier of certification services;

"4. any other relevant factor."

46. The Working Group considered with great interest the proposed new wording for paragraph (4), which was found to introduce elements of particular relevance for assessing the equivalence of certificates in a cross-border context, in particular the reference to recognized international standards. However, various questions were raised as to the meaning of the individual criteria listed and the possible overlap or discrepancies between the new criteria and those already mentioned in draft articles 6, 9 and 10. Also, concerns were voiced that the suggested approach, although having the advantage of being more analytical and focused than the list currently contained in paragraph (4), would render the provision overly complex, thus defeating the purpose of legal clarity. Based on those questions and concerns, the Working Group did not adopt the suggested new wording. As an alternative, it was suggested that essentially the same objective might be achieved by means of cross-references, in paragraph (4), to the appropriate provisions in the uniform rules where the relevant criteria were mentioned, possibly with the addition of other criteria particularly important for cross-border recognition, such as compliance with recognized international standards.

47. It was also pointed out that different criteria could apply to electronic signatures. A proposal for determining substantial equivalence of electronic signatures was made in the following terms:

"In determining whether an electronic signature offers a substantially equivalent level of reliability for the purpose of Article 13(3), regard shall be had to:

"1. whether the means of creating the electronic signature is, within the context in which it is used, linked to the signatory and to no other person;

"2. whether the means of creating the electronic signature was, at the time of signing, under the control of the signatory and of no other person;

"3. whether any alteration to the electronic signature, or any alteration to the

information to which the electronic signature relates, made after the time of signing is detectable;

"4. any recognized international standards applied in relation to the creation of the electronic signature;

"5. any other relevant factor."

48. The Working Group paused to consider the proposed alternatives and examined various ways in which they might be formulated. In the course of its deliberations, however, the Working Group eventually came to the conclusion that an attempt to capture all relevant criteria in one single provision by means of cross-references to earlier portions of the uniform rules was likely to result in a formulation no less complex than the one the Working Group had just discarded.

49. After extensive discussion, and in an effort to bridge the gap between those who advocated eliminating paragraph (4) and those who maintained the importance of the provision, it was decided that paragraph (4) should be redrafted to state that, in determining whether a foreign certificate or an electronic signature offered a substantially equivalent level of reliability for the purposes of paragraphs (2) and (3), regard should be had to recognized international standards and to any other relevant factors. In that connection, it was proposed that the reference to recognized international standards should be replaced by a reference to "international technical and commercial standards" so as to make it clear that the deciding standards were market-driven standards, rather than standards and norms adopted by governmental or intergovernmental bodies. Although that proposal was met with some support, the prevailing view was that it would not be appropriate to exclude governmental standards from among the relevant standards, and that the current formulation was sufficiently broad so as to encompass technical and commercial standards developed by the private sector. It was decided that appropriate explanations should be included in the draft guide to enactment regarding the broad interpretation to be given to the notion of "recognized international standards".

Paragraph (5)

50. The Working Group noted that paragraph (5) originated from an earlier provision (i.e. draft article 19(4) as contained in A/CN.9/WG.IV/WP.73), which recognized the right of Government agencies to specify that a particular certification authority, class of certification authorities or class of certificates must be used in connection with messages or signatures submitted to those agencies. The scope of that provision had been subsequently broadened since the Working Group, when first considering the matter, at its thirty-second session, in 1998, had felt that all parties to commercial and other transactions, and not only Government agencies, should be accorded the same right in connection with messages or signatures they received (A/CN.9/446, para. 207). Noting that it had not since then had the opportunity to examine the provision, the Working Group engaged in an exchange of views on the need for, and desirability of, retaining paragraph (5).

51. In support of keeping the provision, it was said that paragraph (5) reflected a common practice, in particular for transactions involving governmental agencies in some countries, which was aimed at facilitating and supporting standardization of technical requirements. A provision such as paragraph (5) was also important for controlling risks and the potential cost involved in having to test the reliability of unknown certification methods or the trustworthiness of suppliers of certification services that did not belong to a recognized class of certification authorities. Those

costs and risks might be considerable for entities handling a large volume of day-to-day communications with multiple individuals or companies, as was typically the case of governments or financial institutions. Without the possibility of specifying a particular supplier of certification services, class of supplier or class of certificates that they wished to use in connection with messages or signatures submitted to them, those agencies might find themselves under an obligation to accept any class of supplier of certification services or certificate.

52. The prevailing view within the Working Group, however, was that, given the new structure of the draft article, paragraph (5) was not needed and should be deleted. If the purpose of paragraph (5), it was said, consisted in establishing a special prerogative for Government agencies, the provision was unnecessary, since nothing in the uniform rules, which were essentially concerned with commercial transactions, limited or impaired the ability of governments to establish special procedures to be followed in dealing with public administrations. As regards other transactions, however, the classes of suppliers of certification services or certificates to be used were a matter best left for the mutual agreement of the parties concerned. In any event, it would not be appropriate for the uniform rules to appear to be encouraging, or suggesting legislative endorsement of, practices resulting in the unilateral imposition by a private party of a particular certification authority, class of certification authorities or class of certificates. Such a power could lend itself to abuse in the form of discrimination against emerging competitors or industries or other forms of restrictive business practices. Even if paragraph (5) were to be reformulated to provide that the parties might "agree as between themselves", as was suggested, on the use of a particular supplier of certification services, class of supplier or class of certificates, the provision would be redundant, since paragraph (6) already recognized the principle of party autonomy in respect of the choice of certain types of electronic signatures and certificates.

53. After discussion, the Working Group decided that paragraph (5) should be deleted.

Paragraph (6)

54. It was recalled that paragraph (6) was intended to reflect the decision made by the Working Group at its thirty-fifth session that the uniform rules should provide for the recognition of agreements between interested parties regarding the use of certain types of electronic signatures or certificates as sufficient grounds for cross-border recognition (as between those parties) of such agreed signatures or certificates (A/CN.9/465, para. 34). The Working Group based its deliberations on the first alternative wording proposed in paragraph (6) as follows: "Where, notwithstanding paragraphs (2) and (3), parties agree, as between themselves, to the use of certain types of electronic signatures and certificates, that agreement shall be recognized as sufficient for the purpose of cross-border recognition".

55. The view was expressed that paragraph (6) merely restated, in the context of cross-border recognition of electronic signatures and certificates, the principle of party autonomy expressed in draft article 5. Under that interpretation, paragraph (6) was superfluous and potentially damaging since it might create doubts as to the generality of draft article 5. The prevailing view, however, was that paragraph (6) was necessary for the avoidance of doubt, since draft article 12 could be seen as a code relating to cross-border recognition, or could be regarded as a set of mandatory rules, not subject to contractual derogation (for continuation of the discussion with respect to the mandatory nature of the rules, see below, paras. 112-113). In addition, it was stated that specific wording was needed to give effect to contractual

stipulations under which parties would agree, as between themselves, to recognize the use of certain electronic signatures or certificates (that might be regarded as foreign in some or all of the States where the parties might seek legal recognition of a given signature or certificate), without those signatures or certificates being subject to the substantial-equivalence test set forth in paragraphs (2), (3) and (4).

56. A concern was expressed that paragraph (6) might not make it sufficiently clear that, for the purpose of cross-border recognition, the agreement made between the parties should not affect the legal position of third parties. In response, it was generally felt that the words "as between themselves" appropriately reflected the fundamental principle of privity (also referred to as "the relative effect of contracts"), a principle which was readily applicable in most legal systems.

57. It was generally agreed that the recognition of specific agreements under paragraph (6) should be made subject to any mandatory law of the enacting State. A suggestion was to include the following wording, drawn from draft article 5: "unless that agreement would not be valid or effective under the law of the enacting State". While general support was expressed in favour of the policy underlying that suggestion, a concern was raised that the reference to "the law of the enacting State" might be interpreted as interfering unduly with the rules of private international law. While it was explained that the law of the enacting State would inevitably come into play, even if it was only to refer to foreign law through the operation of a rule of conflict, the prevailing view was that, for the purpose of clarity, a reference to "applicable law" should be substituted for the current mention of "the law of the enacting State". It was agreed that the text of draft article 5 should be modified accordingly.

58. After discussion, the Working Group decided that paragraph (6) should read along the following lines: "Where, notwithstanding paragraphs (2), (3) and (4), parties agree, as between themselves, to the use of certain types of electronic signatures or certificates, that agreement shall be recognized as sufficient for the purpose of cross-border recognition, unless that agreement would not be valid or effective under applicable law." The provision was referred to the drafting group, which was also requested to align the text of article 5 with the corresponding wording in paragraph (6). It was generally agreed that appropriate explanations should be inserted in the draft guide to enactment as to the interpretation of the notion of "applicable law".

Article 2. Definitions

59. The text of draft article 2 as considered by the Working Group was as follows:

"For the purposes of these Rules:

"(a) "Electronic signature" means [data in electronic form in, affixed to, or logically associated with, a data message, and] [any method in relation to a data message] that may be used to identify the signature holder in relation to the data message and indicate the signature holder's approval of the information contained in the data message;

"[(b) "Enhanced electronic signature"_ means an electronic signature in respect of which it can be shown, through the use of a [security procedure] [method], that the signature:

"(i) is unique to the signature holder [for the purpose for][within the context in] which it is used;

"(ii) was created and affixed to the data message by the signature holder or using a means under the sole control of the signature holder [and not by any other person];

"[(iii) was created and is linked to the data message to which it relates in a manner which provides reliable assurance as to the integrity of the message";]]

"(c) "Certificate" means a data message or other record which is issued by an information certifier and which purports to ascertain the identity of a person or entity who holds a particular [key pair] [signature device];

"(d) "Data message" means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy;

"(e) "Signature holder" [device holder] [key holder] [subscriber] [signature device holder] [signer] [signatory] means a person by whom, or on whose behalf, an enhanced electronic signature can be created and affixed to a data message;

"(f) "Information certifier" means a person or entity which, in the course of its business, engages in [providing identification services] [certifying information] which [are][is] used to support the use of [enhanced] electronic signatures."

Subparagraph (a) *(Definition of "Electronic signature")*

60. It was recalled that the Working Group, in the context of its discussion of draft article 6 at its previous session, had considered the definition of "electronic signature" and adopted the following wording: "Electronic signature means any method that is used to identify the signature holder in relation to the data message and indicate the signature holder's approval of the information contained in the data message" (A/CN.9/467, paras. 54-58).

"method"

61. Having reviewed that wording, the Working Group was of the view that defining the electronic signature as a "method" was inappropriate, since it created confusion between the process of creating an electronic signature and the result of that process. It was decided that, for continuation of the discussion, the Working Group would instead consider the definition of "electronic signature" contained in document A/CN.9/WG.IV/WP.84 (see above, para. 1) and delete the reference to "method" from that definition.

"approval of the information"

62. Various concerns were expressed about the reference in the definition to the concept of "approval of the information contained in the data message". One concern was that the definition might inappropriately confuse legal and technical concepts. It was suggested that the definition stated in draft article 2 should confine itself to describing the technical characteristics of an electronic signature, for example along the lines of technical definitions adopted by the International Standards Organization (ISO). The legal aspects of electronic signatures should be dealt with only in the operative provisions of the uniform rules, e.g. in draft article 6. A related concern was that the definition might insufficiently reflect the possibility that electronic signatures might be used without any intent of expressing subjective approval of information. In response to those concerns, it was pointed out that defining an electronic signature as capable of indicating approval of information amounted primarily to establishing a technical prerequisite for the recognition

of a given technology as an electronic signature. The legal consequences of applying that technology for signature purposes were dealt with under other draft provisions of the uniform rules. It was also pointed out that the definition did not disregard the fact that technologies commonly referred to as "electronic signatures" could be used for purposes other than creating a legally-significant signature. The definition simply illustrated the focus of the uniform rules on the use of electronic signatures as functional equivalents of hand-written signatures. A suggestion was made that the reference to "approval of information" might be replaced with more general wording to indicate that an electronic signature should be capable of "meeting the legal requirements for a signature". The prevailing view, however, was that the substance of subparagraph (a) should be retained. It was agreed that the draft guide to enactment should make it clear that the notion of "electronic signature" was intended to cover all uses of a handwritten signature for legal effect, the identification of the signatory and the intent to sign being no more than the smallest common denominator to the various approaches to "signature" found in the various legal systems, as already discussed in the context of the preparation of the Model Law. The draft guide should also explain the distinction between the legal notion of "signature" and the technical notion of "electronic signature", a term of art which covered practices that did not necessarily involve the production of legally significant signatures. The draft guide should bring the attention of users to the risk of confusion that might result from the use of the same technical tool for the production of a legally meaningful signature and for other authentication or identification functions.

63. As a matter of drafting, it was agreed that the term "signatory" should be used instead of "signature holder". After discussion, the Working Group decided that subparagraph (a) should be drafted along the lines of "Electronic signature means data in electronic form in, affixed to, or logically associated with, a data message, and that may be used to identify the signatory in relation to the data message and indicate the signatory's approval of the information contained in the data message". The text was referred to the drafting group.

Subparagraph (b) *(Definition of "Enhanced electronic signature")*

64. Consistent with the approach taken by the Working Group at its previous session, it was generally agreed that the current structure of the uniform rules did not make it necessary to use a notion of "enhanced electronic signature" together with the wider notion of "electronic signature", which could receive a more flexible interpretation under draft article 6. The Working Group decided that subparagraph (b) should be deleted.

Subparagraph (c) *(Definition of "Certificate")*

65. A question was raised as to whether a definition of "certificate" was needed, in view of the fact that the meaning of "certificate" as used in the context of certain types of electronic signatures differed little from the general meaning of a document by which a person would confirm certain facts. It was pointed out, however, that the general notion of "certificate" might not exist in all legal systems or indeed in all languages. As a consequence, defining that term in the context of the uniform rules was particularly useful.

"information certifier"

66. As a matter of drafting, it was generally agreed that the term "certification service provider (CSP)" was commonly used in practice and should be preferred to "information certifier", "supplier of certification services" or "certification authority".

"ascertain the identity"

67. Doubts were expressed as to whether the definition should be limited in scope to cover only those certificates known as "identity certificates". In view of the earlier decision by the Working Group that the notion of "identity" should be interpreted broadly so as to cover both designation by name and designation through an attribute of the signatory, it was widely felt that there was no need to limit the scope of the uniform rules to uses of identity certificates. While a certificate could be described generally as authenticating certain information contained in, or logically associated with the certificate, the Working Group agreed that the main function of a certificate in the context of electronic signatures was to provide certainty regarding the existence of a link between a given signature creation device (for example, a private cryptographic key or a biometric indicator) and a signatory. Such linking of a person with a signature creation device was a prerequisite for the operation draft article 9. As to how that function should be expressed in the definition, doubts were expressed regarding the verb "ascertain". A drafting suggestion was to define "certificate" as "a statement establishing a link between a signatory and a signature creation device, which allows confirmation of certain facts relating to an electronic signature". In response to that suggestion, a widely shared view was that the link between the signature creation device and the signatory was not "established" by the certificate, since it was created when the signature creation device was generated. The purpose of the certificate was merely to recognize, show or confirm the link in question. In the context of that discussion, it was agreed that the notion of "signature creation device" should also be defined in draft article 2 (for continuation of the discussion, see below, paras. 70-76).

68. Various drafting improvements were suggested for subparagraph (c). A number of those suggestions included mentioning in the definition of "certificate" that the signature creation device should be "reliable". It was widely felt, in response, that the reliability of the signature creation device (which was dealt with in the substantive provisions of the uniform rules) should be distinguished from the reliability of the link recognized in the certificate. After discussion, the Working Group decided that subparagraph (c) should read along the lines of "Certificate means a data message or other record confirming the link between a signatory and a signature creation device". The text was referred to the drafting group.

Subparagraph (d) *(Definition of "Data message")*

69. It was noted that the definition of "data message" in the uniform rules merely restated the corresponding definition in the Model Law. The Working Group decided that, to ensure consistent interpretation of the two texts, those definitions should be strictly identical. Subparagraph (d) was adopted unchanged. With a view to reflecting technical and commercial developments in the practice of electronic commerce, it was widely felt that "web-based commerce" should be mentioned in the section of the draft guide to enactment corresponding to that definition.

Proposed additional subparagraph *(Definition of "Signature creation device")*

70. In continuation of its earlier discussion of the definition of "certificate" (see above, para. 67), the Working Group considered a possible definition of the notion of "signature creation device".

"Signature creation device" or "signature creation data"

71. As to the nature of the object to be defined, there was general agreement that only one term was needed to designate, throughout the uniform rules, those secret

keys, codes, or other elements that, in the process of creating an electronic signature, were used to provide a secure link between the resulting electronic signature and the person of the signatory. For example, in the context of digital signatures relying on asymmetric cryptography, the core operative element that could be described as "linked to the signatory and to no other person" was the cryptographic key pair. In the context of electronic signatures based on biometric devices, the essential element would be the biometric indicator, such as a fingerprint or retina-scan data. It was widely felt that, in any event, the definition should cover only those core elements that should be kept confidential to ensure the quality of the signature process, to the exclusion of any other element which, although it might contribute to the signature process, could be disclosed without jeopardizing the reliability of the resulting electronic signature. For example, in the case of digital signatures, while both the public and the private key were linked to the person of the signatory, only the private key needed to be covered by the definition, since only the private key should be kept confidential and it was of the essence of the public key to be made available to the public.

72. As to the name of the element to be defined, a widely shared view was that "signature creation device" would appropriately designate the core confidential element on which the signature-creation process was based. However, a concern was expressed that using the term "device" might inadvertently suggest that the defined element should be in the form of hardware, or other physical device. While it was explained that the common usage would define the word "device" as something non-material, such as "an arrangement, scheme, project" or "something devised for bringing about some end or result", the prevailing view was that, in the context of new technologies, the term "device" would probably not be interpreted as connoting the appropriate level of abstraction. The fact that existing international standards might describe "device" as "hardware or software" was not found sufficient to alleviate the above-stated concern, since the desired definition should not encompass any element (e.g. those pieces of hardware or software involved in a "hash function") that might be used in the signature-creation process but would not need to be kept strictly confidential. Among the elements not to be covered by the definition, it was pointed out that the text being electronically signed, although it also played an important role in the signature-creation process, should obviously not be subject to the same confidentiality as the information identifying the signatory. As possible alternatives to "device", the words "code" and "value" were suggested. After discussion, the Working Group decided that, for lack of a better term, the term "signature creation data" should be used.

"Signature creation and signature verification"

73. A question was raised as to whether, alongside a definition of "signature creation data", a definition of "signature verification data" was needed. While the Working Group acknowledged that, particularly in the context of asymmetric cryptography, the signature-creation data (i.e. the private key) was distinct from the signature-verification data (i.e. the public key), it was generally found that draft articles 8 to 10 referred only to those confidential data used for the creation of the electronic signature. Accordingly, it was decided that no definition of "signature-verification data" was needed.

Uniqueness

74. As to the contents of a possible definition of "signature creation data", the following text was proposed: "Signature creation data means data which is unique to the signatory in the context in which it is used, and which can be used to create an electronic signature". Doubts were expressed as to whether a reference to

"uniqueness" could convey the required meaning. The Working Group recalled its deliberations at earlier sessions regarding the concept of "uniqueness". It was pointed out that, in the context of the uniform rules, "uniqueness" should be interpreted as a relative concept. While the private key was unique to the signer, it could be used to produce several electronic signatures; the electronic signature itself might be unique to both the signer and the authenticated message; a hash function and a message digest would also be unique to the message, and yet they would not need to be kept confidential. With a view to alleviating some of the difficulties linked to that notion of "uniqueness", the following wording was suggested, among various possible wordings that borrowed from draft article 6: "Signature creation data means data which can be used to create an electronic signature and, in that context, is linked to the signatory and to no other person". In the discussion of that suggestion, a more general concern was expressed that dealing with the exclusive link between the signature creation data and the signatory was a function of draft article 6, which should not be made part of the definition of "signature creation data". A proposal was made for a minimalist definition along the lines of "signature creation data means data used for the creation of an electronic signature". At that stage, doubts were expressed as to the usefulness of including in the uniform rules a definition that merely stated the obvious.

75. General preference was expressed for not having the definition and relying on draft article 6 to express the idea that the signature creation data should be linked to the signatory and to no other person. While it was generally agreed that the notion of "signature creation data" should be used throughout the text as a self-explanatory notion, a question was raised as to whether the reference in draft article 6(3) to "the means of creating the electronic signature" should be replaced by a reference to "the signature creation data". It was widely felt that, in the context of a general description of the means that were used at the time and for the purpose of creating the electronic signature, elements of data, hardware or software other than the core secret data envisaged in draft articles 8 to 10 might also need to be under the exclusive control of the signatory (for continuation of the discussion, see below, para. 144).

76. After discussion, the Working Group decided that no definition of "signature creation device" or "signature creation data" was needed. In the text of the uniform rules, the term "signature device" should be replaced by the term "signature creation data". In draft article 6, the reference to "the means of creating an electronic signature" should be maintained. The draft guide to enactment should make it clear that in the uniform rules, "signature creation data" was intended to cover only the private cryptographic key (or other confidential data linked to the identity of the signatory) that was used to create an electronic signature. Should other data (such as the text to be authenticated) be used in the process of creating the electronic signature (through a hash function or otherwise), those data should not be covered by the obligations set forth in draft article 8, since keeping those data confidential was not essential to guarantee the reliability of the electronic signature process. The text was referred to the drafting group.

Subparagraph (e) *(Definition of "Signatory")*

77. In line with its earlier decision to use the word "signatory" (see above, para. 63), the Working Group decided to remove the square brackets around that word and to delete all alternative expressions contained in subparagraph (e).

78. Noting its earlier decision to delete the definition of "enhanced electronic signature" (see above, para. 64), the Working Group decided to delete the word "enhanced" in subparagraph (e). In that connection, it was pointed out that, as the

uniform rules no longer distinguished between electronic signatures and enhanced electronic signatures, the duties and obligations of signatories, relying parties and certification service providers set forth in the uniform rules applied with respect to all classes and types of certificates and electronic signatures. Those duties and obligations, it was said, might be appropriate in connection with high-value certificates or electronic signatures of the type previously referred to as "enhanced electronic signatures". However, those duties and obligations might be excessive with respect to low-value certificates or electronic signatures offering a lesser degree of security, whose issuers and users should not be expected to have to comply with all the requirements of articles 8 and 9. One suggestion to counter that problem was to restrict the definition of "signatory" by limiting it to persons by whom or on whose behalf "legally required signatures" could be created.

79. The Working Group was generally of the view that the degree of trustworthiness offered by a certificate should normally be commensurate with the purposes for which the certificate was used and that certificates or electronic signatures sometimes used in practice were not always intended to be legally relevant. The example was given of situations where an electronic signature would be used for authenticating a browser. However, the Working Group, did not accept the proposed amendment to subparagraph (e), since the prevailing view was that it would not be appropriate to limit the concept of "signatory", which was used throughout the uniform rules, by reference to the purpose for which an electronic signature was used.

"can be created"

80. The view was expressed that, in practice, a person could not become a signatory before he or she had actually used the signature creation data to produce an electronic signature. Since the reference, in the definition, to a person by whom an electronic signature "can be created" only denoted the possibility or ability to create a signature, it would be more appropriate to use words such as "is created" or any other phrase of equivalent meaning.

81. In response, it was pointed out that draft Article 8 established specific obligations for the signatory in respect of the contents of certificates and the use or condition of signature creation data, which were not necessarily connected, with the act of creating an electronic signature. Obligations such as the obligations to exercise reasonable care to avoid unauthorized use of the signature creation data (draft Article 8(1)(a)) or to notify the relying party if the signature creation data was known to have been compromised (draft Article 8(2)(i)), for instance, were relevant both before and after the electronic signature was created.

"by whom or on whose behalf"

82. The Working Group considered several questions raised in connection with the use of the phrase "by whom or on whose behalf" in subparagraph (e) and the implications that the use of such phrase had for the definition of "signatory", as used in the uniform rules.

83. Pursuant to one view, that phrase was not adequate in the context of subparagraph (e), since the quality of "signatory" was inherently that of the person that actually created the electronic signature, irrespective of whether that person acted on its own account, or on behalf of someone else. Tracing a parallel to the use of hand-written signatures, it was pointed out that a person that signed a contract as an agent for another person was still regarded as the signatory of the contract, even though the contract was to become binding on the person whom he or she was representing.

84. Another view was that, in the context of the uniform rules, the deciding factor for conferring the quality of signatory upon a person was the attribution of the signature to that person, even though the signature was in fact generated by an agent. In that sense, the use of the phrase "by whom or on whose behalf" in subparagraph (e) was correct and should be retained. Another view was that the phrase should read "or by whose authority". Yet another view, which took an intermediate position between the other interpretations, was that, in the context of communications by electronic means, the notion of signatory might need to be defined in a manner that encompassed both the person that actually generated the electronic signature and the person to whom the signature was attributed.

85. The analogy to hand-written signatures, it was stated, was in principle acceptable, but might not always be suitable for taking advantage of the possibilities offered by modern technology. In a paper-based environment, for instance, legal entities could not strictly speaking be signatories of documents drawn up on their behalf, because only natural persons could produce authentic hand-written signatures. Electronic signatures, in turn, could be conceived so as to be attributable to companies, or other legal entities (including governmental and other public authorities), and there might be situations where the identity of the person who actually generated the signature, where human action was required, might not be relevant for the purposes for which the signature was created. Recent measures to improve and modernize domestic tax collection and administration systems in some jurisdictions were already taking advantage of that possibility by assigning signature creation data to legal entities, rather than to the individuals acting on their behalf. The definition of "signatory" in the uniform rules, it was said, should be flexible enough to acknowledge those practices.

86. The Working Group considered at length the various views that had been expressed. In the context of that discussion, the Working Group generally agreed that, consistent with the approach taken in the Model Law, any reference in the uniform rules to a "person" should be understood as covering all types of persons or entities, whether physical, corporate or other legal persons. The Working Group was sympathetic to the need for affording a sufficient degree of flexibility to the definition so as not to pose obstacles to the use of electronic signatures in the manner most suitable in a paperless environment. The Working Group was nevertheless of the view that the notion of signatory for the purposes of the uniform rules could not be severed from the person or entity that actually generated the electronic signature, since a number of specific obligations of the signatory under the uniform rules were logically linked to actual control over the signature creation data. However, in order to cover situations where the signatory would be acting in representation of another person, the phrase "or on whose behalf" or another equivalent phrase, should be retained in the definition of "signatory".

87. It was the understanding of the Working Group that the extent to which a person would be bound by an electronic signature generated "on its behalf" was a matter to be settled in accordance with the law governing, as appropriate, the legal relationship between the signatory and the person on whose behalf the signature was generated, on the one hand, and the relying party, on the other hand. That matter, as well as other matters pertaining to the underlying transaction, including issues of agency and other questions as to who bore the ultimate liability for failure by the signatory to comply with its obligations under article 8 (whether the signatory or the person represented by the signatory) were outside the scope of the uniform rules.

88. Concluding its deliberations on this topic, the Working Group decided that "signatory" should be defined as a person that holds signature creation data and acts either on its own behalf or on behalf of the person it represents, and referred

subparagraph (e) to the drafting group.

Subparagraph (f) *(Definition of "Certification services provider")*

89. As a matter of drafting, the Working Group decided to use the expression "certification services provider" instead of "information certifier", "supplier of certification services" or "certification authority" (see above, para. 66)). Noting also its earlier decision to delete the definition of "enhanced electronic signature" (see above, para. 64), the Working Group decided to delete the word "enhanced" in subparagraph (f).

90. The suggestion was made that, since the main functions of certification service providers that were relevant for the uniform rules were set out in draft article 9, and since the notion of certification service provider was not used elsewhere in the uniform rules, the definition was not needed and might be deleted. In support of that suggestion, it was said that the only additional element of practical significance contained in subparagraph (f) was the qualification of a certification service provider as a person or entity that provided those services "in the course of its business". However, no separate provision was required only for expressing that qualification, since the same result might be achieved, for instance, by inserting the phrase "in the course of its business" at an appropriate place in the *chapeau* of draft article 9.

91. The Working Group was sensitive to the aim of economy of language in drafting the uniform rules. Nevertheless, the Working Group decided that, since subparagraph (e) defined the notion of "signatory", the definition of certification service provider should be retained in order to ensure symmetry in the definition of the various parties involved in the operation of electronic signature schemes under the uniform rules.

"in the course of its business"

92. The Working Group considered various questions that were raised in connection with the meaning of the words "in the course of its business", which was found to contain some ambiguity.

93. There was general agreement within the Working Group that a person or entity whose main activity was the provision of certification services, in particular the issuance of certificates, carried out that activity "in the course of its business" and should, therefore, be covered by the definition of certification service provider under the uniform rules. However, that formulation was felt to create some difficulties. The word "business" might not be broad enough to cover the commercial activities of public authorities or non-profit organizations. In addition, the duties of certification service providers under draft article 9 resulted from the performance of a variety of functions, not all of which were in the nature of certification (such as, for example, managing and maintaining a list of revoked certificates). Furthermore, certain of those ancillary or complementary functions might not be carried out by the certification service provider itself. In practice, a number of such functions might be contracted out to other persons or entities whose main activity might not be the provision of certification services.

Certification service provider and subcontractors

94. The question was asked whether, in such cases, only the issuer of certificates would become a "certification service provider" for the purposes of the uniform rules, or whether all subcontractors and other persons or entities should come under the definition of subparagraph (f). The latter situation, it was said, might have undesirable consequences, since the provisions of article 9 were developed essentially

for persons or entities whose main activity was the provision of certification services.

95. In considering that question, the Working Group took the view that the possibility of multiple parties performing functions relevant for the purposes of draft article 9 did not pose a problem for the definition of certification service provider. When other parties performed services in connection with certificates issued by a certification service provider, they did so either as independent certification service providers of their own right, or as subcontractors of a certification service provider. In the first case, those other parties would be automatically subject to the provisions of article 9. In the second case, they would be regarded as agents of the certification service providers, and the manner in which their duties and liability under draft article 9 was allocated was a matter to be dealt with in their contractual arrangements with the certification service provider. Neither of those cases would, in the view of the Working Group, affect the rights of the relying party under draft article 9.

Issuance of certificates on a habitual or an occasional basis

96. The Working Group focused its attention on other questions raised by the phrase "in the course of its business". In favour of retaining that phrase in subparagraph (f), it was said that a certain element of regularity in the performance of certification services was needed, in order for person or entity to be required to comply with article 9. Without that qualification in subparagraph (f) the definition of certification service provider would encompass even persons or entities who only occasionally or incidentally provided certification services or issued certificates, as in some of the examples given.

97. The countervailing view was that, in practice, the likelihood that a person or entity might be in a position to provide certification services sporadically was not a significant one, in view of the cost entailed by equipping itself for that purpose. If excluding such occasional providers of certification services was the only purpose of the phrase "in the course of its business", that phrase had little practical value, and could be deleted. Moreover, if the intention was to circumscribe the application of the uniform rules to the use of certificates and electronic signatures in particular situations, alternative wording should be used, since the phrase in question was not sufficiently clear for that purpose.

Issuance of certificates as a main or a secondary activity

98. Indeed, one possible interpretation of the phrase "in the course of its business" might be that the uniform rules applied only to those entities whose main activity was the provision of certification services. Another interpretation might be that a person or entity that issued certificates would still be regarded as a certification service provider, for the purposes of the uniform rules, even if its main activity was not the provision of certification services, as long as such person or entity issued the certificates "in the course of its business". Examples brought to the attention of the Working Group included companies that issued certificates that their employees might use in dealing with social security and welfare bodies; health insurance companies that issued certificates to be used by their customers in dealings with third parties; or governmental organs that certified public keys used to verify digital signatures created by other governmental agencies. If the first interpretation of the words "in the course of its business" in subparagraph (f) was correct, none of those companies, insurers or governmental organs could be regarded as certification service providers, since the provision of certification services was not their main activity. If, in turn, the second interpretation was correct, those companies, insurers or governmental organs might well qualify as certification service providers, since the issuance of certificates occurred "in the course of their business".

99. After an extensive debate on the matter, and having considered the various views that had been expressed, the Working Group decided that the phrase "in the course of its business" should be deleted. In reaching that decision, the Working Group noted that, pursuant to draft article 1, the uniform rules would apply to the use of electronic signatures in the context of commercial transactions. It was the understanding of the Working Group that, in view of that limitation in the scope of application of the uniform rules, entities that issued certificates for internal purposes and not for commercial purposes would not fall under the category "certification service providers" for the purposes of the uniform rules. That interpretation should be reflected clearly in the draft guide to enactment of the uniform rules.

100. In the deliberations, it was decided that the definition of "certification service provider" should emphasize that, in all cases, the certification service provider as defined would have to provide certification services, possibly together with other services. The Working Group concluded its deliberations on the matter by deciding that the current definition of "information certifier" should be replaced with a definition along the following lines: "'Certification service provider' means a person that issues certificates and may provide other services related to electronic signatures." The provision was referred to the drafting group.

Proposed definition of "recognized international standards"

101. The suggestion was made that the uniform rules should include a definition of "recognized international standards", an expression which was used in connection with the recognition of foreign certificates and electronic signatures (see above, paras. 46-49). The following wording was proposed:

> "Recognized international standards means statement of accepted technical, legal or commercial practices, whether developed by the public or private sector [or both], of a normative or interpretative nature which are generally accepted as applicable internationally. Without limiting its generality, such standards may be in the form of requirements, recommendations, guidelines, codes of conduct, or statements of either best practices or norms."

102. It was pointed out that the proposed definition was consistent with the understanding thus far given by the Working Group to the term "standard", which had been interpreted in a broad sense so as to include industry practices and trade usages, texts emanating from international governmental or non-governmental organizations.

103. While strong support was expressed to the proposed definition, the prevailing view was that the matter should best be left for the draft guide to enactment, rather than to the body of the uniform rules. It was pointed out that some jurisdictions had established rules governing the hierarchy of international norms, which often gave precedence, in case of conflict, to norms contained in international agreements or which emanated from public international organizations. While it might be useful to remind judges and other authorities involved in the application of the uniform rules of the importance of taking duly into account the standards developed by private sector organizations, it would not be appropriate for the uniform rules to appear to interfere with the rules of the enacting State on the hierarchy of sources of law. It was pointed out, in that connection, that the notion of "general principles", which was used in draft article 4(2) was not the object of a specific definition. That approach was found to be consistent with the approach that had been taken in article 3(2) of the Model Law, which used the same expression, but left the explanation of its meaning to its guide to enactment. Furthermore, the proposed definition left open the question of what constituted "recognition" and of whom such recognition was required.

104. Having considered the different views that were expressed, the Working Group decided that the proposed definition should not be included in the text of the uniform rules, but that an appropriate explanation of the meaning of the expression "recognized international standards", which captured the essential elements of the proposed definition, should be added to the current wording of the draft guide to enactment.

Proposed definition of "relying party"

105. The proposal was made that the uniform rules should contain a definition of the term "relying party", which although used in various places in the uniform rules, was not frequently used in many jurisdictions.

106. Various objections were expressed on that proposal in view of the perceived difficulty of formulating it with the level of conciseness and generality that would be required to cover all situations in which a party might rely on an electronic signature or on the information contained in a certificate.

107. The Working Group took the view, however, that such a definition would be useful in order to ensure symmetry in the definition of the various parties involved in the operation of electronic signature schemes under the uniform rules. The Working Group decided that "relying party" should be defined as "a person that may act on the basis of a certificate or an electronic signature" and referred the matter to the drafting group.

108. In the context of that discussion, a concern was expressed that, in certain legal systems, the adopted wording ("a person may act") would insufficiently cover the situation where an omission (as opposed to an "action") would be the result of the party's reliance on the certificate or the electronic signature. It was proposed that the words "a person that may act or commit an omission" should replace the words "a person that may act" in the definition of "relying party". After discussion, however, it was generally agreed that the above-mentioned concern would sufficiently be taken care of it the draft guide to enactment was to make it clear that, for the purposes of that definition, "act" should be interpreted broadly to cover not only a positive action but also an omission.

109. Having concluded its deliberations regarding draft articles 2 and 12, the Working Group proceeded to review the remainder of the provisions contained in the uniform rules to consider matters that had remained unsettled at the end of the thirty-sixth session of the Working Group. Possible changes to be introduced in the text as a result of the decisions taken at the current session were also discussed.

Article 5. Variation by agreement

110. The text of draft article 5 as considered by the Working Group was as follows:

> "These Rules may be derogated from or their effect may be varied by agreement, unless that agreement would not be valid or effective under the law of the enacting State [or unless otherwise provided for in these Rules]."

111. The Working Group noted that the substance of draft article 5 had been adopted by the Working Group at its thirty-sixth session (New York, 14-25 February 2000), except for the words within square brackets "unless otherwise provided in these Rules", which were retained in the draft article pending a decision as to whether the uniform rules would contain any mandatory provision (A/CN.9/467, para. 40).

112. Having considered the matter once more, the Working Group decided to delete the words within square brackets, as it was generally agreed that the uniform rules, as currently formulated, did not contain any mandatory provision. It was understood that the principle of party autonomy applied also in the context of article 13(1). Therefore, although the courts of the enacting State or authorities responsible for the application of the uniform rules should not deny or nullify the legal effects of a foreign certificate only on the basis of the place where the certificate was issued, article 13(1) did not limit the freedom of the parties to a commercial transaction to agree on the use of certificates that originated from a particular place.

113. In the context of that discussion, a concern was expressed that the effect of draft article 5, if read in combination with draft article 6(1), might be inconsistent with that of the corresponding provisions of the Model Law (i.e. articles 4(2) and 7(1) of the Model Law). It was stated that if the uniform rules were to provide for broad recognition of contractual derogations, they might contradict the Model Law, which provided for limited recognition of party autonomy with respect to mandatory requirement for hand-written signatures that might exist in applicable law. In response to that concern, it was explained that the recognition of contractual derogations to the uniform rules under draft article 5 was equally subject to the mandatory rules of applicable law, even if the wording of the uniform rules was not strictly modelled on that of the Model Law in that respect.

Article 9. Conduct of the certification service provider

114. The text of draft article 9 as considered by the Working Group was as follows:

"(1) A supplier of certification services shall:

"(a) act in accordance with representations made by it with respect to its policies and practices;

"(b) exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life-cycle, or which are included in the certificate;

"(c) provide reasonably accessible means which enable a relying party to ascertain from the certificate:

"(i) the identity of the supplier of certification services;

"(ii) that the person who is identified in the certificate had control of the signature device at the time of signing;

"(iii) that the signature device was operational on or before the date when the certificate was issued;

"(d) provide reasonably accessible means which enable a relying party to ascertain, where relevant, from the certificate or otherwise:

"(i) the method used to identify the signatory;

"(ii) any limitation on the purpose or value for which the signature device or the certificate may be used;

"(iii) that the signature device is operational and has not been

compromised;

"(iv) any limitation on the scope or extent of liability stipulated by the supplier of certification services;

"(v) whether means exist for the signatory to give notice that a signature device has been compromised;

"(vi) whether a timely revocation service is offered;

"(e) provide a means for a signatory to give notice that a signature device has been compromised, and ensure the availability of a timely revocation service;

"(f) utilize trustworthy systems, procedures and human resources in performing its services.

"(2) A supplier of certification services shall be liable for its failure to satisfy the requirements of paragraph (1)."

General remarks

115. The Working Group was reminded of its earlier discussion concerning the implications of the deletion of the definition of "enhanced electronic signature", and of the concerns that had been expressed that the duties and obligations of signatories, relying parties and certification service providers now applied with respect to all classes and types of certificates and electronic signatures, irrespective of their particular level of reliability (see above, paras. 78-79). That situation, it was said, was unsatisfactory, since it was not reasonable to subject so-called "low value certificates" (which were merely declaratory in nature and were not intended to support the creation of legally recognized electronic signatures), to substantially the same regime as that governing the type of certificates that would be used in connection with electronic signatures meant to satisfy the requirements of draft article 6.

116. In order to avoid those difficulties, the Working Group was urged to adjust the sphere of application of draft articles 8 and 9 by linking those provisions to draft article 6. It was proposed that opening clauses should be added in draft articles 8 and 9 to the effect that they would only apply where the signatory intended to create an electronic signature that complied with draft article 6 or when a certification service provider rendered services intended to support the creation of such an electronic signature.

117. The Working Group was generally in agreement with the view that it would not be appropriate to require from a signatory or a certification service provider a degree of diligence or trustworthiness that bore no reasonable relationship to the purposes for which the electronic signature or certificate was used. Although the view was expressed that the duties and obligations provided in draft article 9 could reasonably be expected to be complied with by any certification service provider, and not only those who issued "high value" certificates, the Working Group favoured a solution which linked the obligations set forth in both articles 8 and 9 to the production of legally-significant electronic signatures.

118. Having considered various options, the Working Group expressed a preference for formulations that avoided reference to the intention of the signatory to create a legally-recognized electronic signature or to create a signature that produced legal effects. It was generally felt that the signatory's intention might not be easily

ascertained in concrete situations. It was further pointed out that there were situations in which a signature might become legally relevant despite the absence of a corresponding intention on the part of the signatory. Moreover, the question of whether and to what extent a particular type of electronic signature had legal effects in a given jurisdiction was a matter for the applicable law and not merely a function of the signatory's intention.

119. After deliberation, the Working Group decided that a phrase along the following lines should be added at the beginning of draft article 8: "Where signature creation data can be used to create an electronic signature that has legal effect [...]". The Working Group further decided that a phrase such as "Where a certification service provider provides services to support an electronic signature that may be used for legal effect as a signature [...]" should be added at the beginning of draft article 9. The Working Group referred the matter to the drafting group. It was stated that the draft guide to enactment should mention that the additional phrases were not intended to create new types of legal affects for signatures.

Subparagraph (1)(c)

120. In connection with subparagraph (1)(c)(ii), the view was expressed that it would not be appropriate to require the certification service provider to offer "reasonably accessible means which enabled a relying party to ascertain from the certificate that the person who is identified in the certificate has control of the signature creation date at the time of signing". It was pointed out that a certification service provider could only be expected to state the identity of the holder of the signature creation device, but had no means of establishing whether that person was in fact in control of the signature creation data at the time of signing. If the wording of subparagraph (1)(c)(ii) was retained, that provision could be construed as establishing a strict liability of the certification service provider for damage sustained by the relying party as a result of the misuse of a signature creation device by an unauthorized person. Therefore, the proposal was made that the current words in subparagraph (1)(c)(ii) should be deleted and replaced with "the identity of the signatory at the time the certificate was issued".

121. A countervailing view was that the proposed amendment was not necessary, since the rule contained in subparagraph (1)(c)(ii) did not require the certification service provider to guarantee that the person who was identified in the certificate had control of the signature creation date at the time of signing. In fact, subparagraph (1)(c)(ii) only required the certification service provider to offer "reasonably accessible means" which enabled the relying party to establish those facts. The provision, as currently drafted, was a logical consequence of the reliability test established in draft article 6(3)(b) and represented the only practical avenue offered to the relying party to assess the reliability of an electronic signature.

122. In considering those views, the Working Group was sympathetic to the objective of offering the relying party the best possible means, as appropriate in the circumstances, for assessing the reliability of an electronic signature. The most important of those means was indeed the identity of the signatory, which was related to the actual control of the signature creation data. However, it was generally felt that a certification service provider could only be expected to state the identity of the person who held the signature creation data at the time a certificate was issued. For this purpose, the Working Group did not treat the word "control" as differing in meaning from the word "hold". Subparagraph (1)(c)(ii) was not intended to require certification service providers to develop means of tracing a signature creation device after a certificate was issued or to control the conduct of the holder of such data. Such an obligation, even if it were feasible in practice, would place an unreasonable burden

upon certification service providers.

123. The Working Group recognized, however, that the current wording of the subparagraph might lend itself to misunderstanding and decided, after deliberation, that it should be reformulated so as to refer to the "signatory" having "control of the signature creation data at the time when the certificate was issued". With that understanding, the matter was referred to the drafting group.

Subparagraph (1)(d)

124. It was pointed out that the signatory's duty to give notice regarding compromised signature creation data under draft article 8(b) covered both cases where the signatory knew that the signature creation data had been compromised and cases where the circumstances known to the signatory gave rise to a substantial risk that the signature data might have been compromised. Subparagraph (1)(d)(v), however, only required the certification service provider to offer reasonably accessible means which enabled a relying party to ascertain whether there were means for the signatory to give notice that a signature device had been compromised. Thus, the current wording of draft article 9(1)(d)(v) did not appear to cover all situations referred to in draft article 8(1)(b). Noting that the same lack of symmetry existed between draft article 9(e) and draft article 8(1)(b), the Working Group decided that both subparagraphs (d)(v) and (e) should be aligned with draft Article 8(1)(b), and referred the matter to the drafting group.

125. In connection with subparagraph (1)(d), the concern was expressed that the provision might impose upon the certification service provider the obligation to maintain lists of possibly compromised signature creation data or to issue notices in connection with notices to that effect received from signatories. It was pointed out that, in practice, certifications services providers maintained lists of revoked certificates, but not other types of lists as might be implied in subparagraph (1)(b). In response, it was recalled that paragraph (1) only required the certification service provider to offer reasonably accessible means which enabled a relying party to ascertain, where relevant, from the certificate or otherwise whether means existed for a signatory to give the notices in question. The only obligation created by that provision was to provide information as to the existence, if any, of those means, which was further made clear by the use of the words "where relevant".

Subparagraph (1)(e)

126. The view was expressed that subparagraph (1)(e) appeared to suggest that a certification service provider, regardless of the category of certificates it issued, was under the obligation to provide means for the signatory to give notice that a signature creation data had been compromised, and to ensure the availability of a timely revocation service. If that was so, subparagraph (1)(e) was not entirely consistent with subparagraph (1)(d)(v) and (vi), from which it could be inferred that such facilities might not always be provided.

127. The Working Group was of the view that subparagraph (1)(e) was not intended to apply to certificates such as transactional certificates (which are one-time certificates) or other types of certificates that might not be subject to revocation. Thus, the Working Group agreed that the obligations of the certification service provider under subparagraph (1)(e) were not absolute, but applied only where such services were made available to the signatory, whether directly by the certification service provider or indirectly through an intermediary. It was therefore decided that the drafting group should revise the language of subparagraph (1)(e) with a view to ensuring its consistency with subparagraph (1)(d)(v) and (vi).

Article 10. Trustworthiness

128. The text of draft article 10 as considered by the Working Group was as follows:

"[In determining whether and the extent to which any systems, procedures and human resources utilized by a supplier of certification services are trustworthy, regard shall be had to the following factors:

"(a) financial and human resources, including existence of assets;

"(b) quality of hardware and software systems;

"(c) procedures for processing of certificates and applications for certificates and retention of records;

"(d) availability of information to signatories identified in certificates and to potential relying parties;

"(e) regularity and extent of audit by an independent body;

"(f) the existence of a declaration by the State, an accreditation body or the supplier of certification services regarding compliance with or existence of the foregoing; and

"(g) any other relevant factor.]"

129. The Working Group engaged in a discussion as to whether article 10 should be retained in the body of the uniform rules, or whether the substance of the provision should be included in the draft guide to enactment.

130. In favour of retaining draft article 10, it was stated that the provision offered useful guidance to assist with the interpretation of the notion of "trustworthy systems, procedures and human resources" in article 9(1)(f). It was also pointed out that a similar list, which had originally been contained in an earlier version of draft article 12, had been deleted by the Working Group, among other reasons because its elements were already contained in draft article 10. If the draft article, too, was deleted the courts of the enacting State and other authorities responsible for the application of the uniform rules would be left with no guidance to assess whether, in a given case, the requirements of article 9(1)(f) had been met.

131. In favour of removing the substance of the draft article and placing it in the draft guide to enactment, it was stated that the draft article merely elaborated on a matter dealt with only in draft article 9(1)(f) and nowhere else in the uniform rules. Furthermore, the elements listed in the draft article set a standard of trustworthiness which, while appropriate in connection with the type of electronic signatures previously referred to as "enhanced electronic signatures", might be too high for issuers of low-value certificates.

132. The Working Group noted that draft article 10 contained a non-exhaustive list of factors to be taken into account in determining trustworthiness. That list was intended to provide a flexible notion of trustworthiness, which could vary in content depending upon what was expected of the certificate in the context in which it was created. In view of the flexible formulation used in the draft article, the standard set therein provided a reasonable level of trustworthiness and was not as stringent as the standards set in some jurisdictions for assessing the trustworthiness of persons or entities that issued certificates to be used in connection with the type of electronic

signatures previously referred to by the Working Group as "enhanced electronic signatures". Moreover, the amendments that had been introduced by the Working Group in the *chapeaux* of draft articles 8 and 9 (see above, paras. 117-119) had already taken into account the particular situation of certification service providers that issued low-value certificates and for whom the requirements of draft articles 9 and 10 might be excessive.

133. The Working Group concluded its deliberation by deciding to remove the square brackets around draft article 10 and requested the drafting group to consider whether, for ease of reading, the provision should be retained as a separate article, or whether it should be incorporated into draft article 9. With a view to emphasizing the non-exhaustive nature of the list set forth in draft article 10, it was decided that the words "regard shall be had" should be replaced by the words "regard may be had", while the conjunction "or" should be substituted for "and" at the end of subparagraph (f).

C. Form of the instrument

134. Having concluded its consideration of the individual provisions contained in the uniform rules, the Working Group proceeded to consider the appropriate form that should be given to the rules.

135. The Working Group noted that, in the course of the preparation of the uniform rules, different approaches had been suggested as to what the form might be, which included contractual rules, legislative provisions, or guidelines for States considering enacting legislation on electronic signatures. The Working Group also noted that it had been agreed as a working assumption that the uniform rules should be prepared as legislative rules with commentary, and not merely as guidelines (see A/CN.9/437, para. 27; A/CN.9/446, para. 25; and A/CN.9/457, paras. 51 and 72). Since no suggestion had been made that the uniform rules should take the form of an international convention, the options offered for the consideration of the Working Group, at the current stage, were essentially to present the instrument as a model law, to retain the denomination "uniform rules", or to use the title "model legislative provisions".

136. In favour of retaining the denomination "uniform rules", or using a title such as "model legislative provisions", it was recalled that the uniform rules had been prepared on the assumption that they should be directly derived from article 7 of the Model Law and should be considered as a way to provide detailed information as to the concept of a reliable "method used to identify" a person and "to indicate that person's approval" of the information contained in a data message (see A/CN.9/WG.IV/WP.71, para. 49). Such a denomination would facilitate understanding of the relationship between the uniform rules and the Model Law, as well as the incorporation of the uniform rules in the legal systems of enacting States. Indeed, the relationship between the uniform rules and the Model Law was analogous to the relationship that existed in many legal systems between a statute and its implementing regulations.

137. In favour of calling the instrument a "model law", it was said that the title "rules", as used in the practice of UNCITRAL, had thus far been reserved to instruments of a contractual nature which, rather than being addressed to legislators, were offered to parties for incorporation into their contracts. Prominent examples were the UNCITRAL Arbitration Rules (1976) and the UNCITRAL Conciliation Rules (1980). To the extent that the uniform rules represented a legislative text that was recommended to States for adoption as part of their national law, the title "model law" would be more appropriate. The word "law", in that context, was not equivalent

to "statute", and did not express a recommendation concerning the form or hierarchy of the instrument which each enacting State might choose for enacting it. Those States that had already enacted general statutes on electronic commerce or that wished to do so, but preferred to issue regulations on electronic signatures under the authority of such general statutes, would in no way be hindered in proceeding as they saw fit.

138. After considering the various options, the Working Group decided to suggest to the Commission that the instrument, once adopted, should bear the title "UNCITRAL Model Law on Electronic Signatures".

D. Relationship with the UNCITRAL Model Law on Electronic Commerce

139. The Working Group was reminded of the close relationship between the draft Model Law on Electronic Signatures, and the UNCITRAL Model Law on Electronic Commerce, in particular with article 7 of the latter text. In that connection, the view was expressed that the Working Group should consider ways in which that relationship might be highlighted, with a view to avoiding the appearance that the two instruments were entirely unrelated to one another.

140. One such possibility might be to incorporate the provisions of draft Model Law on Electronic Signatures in an extended version of the Model Law, for example to form a new part III of the Model Law. However, that possibility was discarded by the Working Group in view of the practical difficulty of combining the two instruments in one single text.

141. Another possibility considered by the Working Group was to formulate a preamble, which would clearly state that the Model Law on Electronic Signatures had been prepared by the Commission to implement article 7 of the Model Law on Electronic Commerce. While the Working Group saw some attractiveness in the proposal, it was decided that a preamble might not be necessary, if its sole content was a statement of that nature.

142. The Working Group noted that, as was customary for most instruments produced by the Commission, the Model Law on Electronic Commerce, in its published version, was preceded by a text reproducing the resolution of the General Assembly in which the Assembly, *inter alia*, recommended that all States should give favourable consideration to the Model Law when they enacted or revised their laws. As it was expected that the General Assembly might wish to adopt a similar resolution in respect of the Model Law on Electronic Signatures, following its finalization and adoption by the Commission, the Working Group was of the view that such a resolution might offer an appropriate context for highlighting the relationship between the two model laws.

E. Report of the drafting group

143. Having completed its consideration of the substance of the draft provisions of the draft Model Law, the Working Group requested the Secretariat to establish a drafting group to review the entire text with a view to ensure consistency between the various draft articles in the various language versions.

144. In reviewing the report of the drafting group, the Working Group noted that, consistent with the decision taken by the Working Group with respect to the definition of "signature creation data" (see above, paras. 75-76), the drafting group had maintained the reference to "the means of creating the electronic signature in draft

article 6(3)(a) and (b). Doubts were expressed as to whether maintaining such a dual terminology was necessary. Having given in-depth consideration to both subparagraphs (a) and (b) of draft article 6, the Working Group came to the conclusion that, at least in the context of subparagraph (a), there was no inconvenience in replacing the term "means of creating the electronic signature" by "signature creation data", since the signature creation data was precisely the factor used to establish the link between the electronic signature and the person of the signatory. The situation under subparagraph (b) was more difficult. It was widely understood that, at the time of signing, the reliability of the electronic signature would depend not only on the signatory having control of the signature creation data (e.g., its private key) but also on control of the hardware and software environment that came into play when applying the signature creation data. In that context, a reference to such a concept as "signature creation device" (or a broad interpretation of the notion of "signature creation data") might be justified to reflect the fact that the signature creation data and the environment in which they were applied to create the electronic signature were equally critical to the reliability of the signature-creation process. While that fact was largely admitted, the Working Group was mindful of the difficulty that might be created if the notion of "signature creation data" were to be given a broad interpretation in the context of draft article 6(3)(b) and a narrow interpretation in the remainder of the draft Model Law. After discussion, the Working Group decided that the term "signature creation data" should be used throughout the uniform rules, including draft article 6(3)(a) and (b), and should be given consistently the narrow interpretation decided upon in the earlier part of the discussion (see above, para. 76). As a reason for not covering in draft article 6(3)(b) the hardware and software environment in which the signature creation data were applied, it was stated that the signatory could be expected to exercise control over the signature creation data but not necessarily over its hardware and software environment.

III Draft guide to enactment

A. General remarks

145. The Working Group expressed overall satisfaction with the structure and contents of the draft guide to enactment contained in documents A/CN.9/WG.IV/WP.86 and Add.1.

146. Various views were expressed as to the appropriateness of maintaining in the draft guide a relatively long account of the history of the preparation of the draft Model Law. One view was that such a historical report should be deleted as unnecessary. Another view was that its length should be considerably reduced. Yet another view was that it should be placed in an annex to the document. A widely shared view, however, was that, in a number of countries, such a record of the history would be regarded as useful by legislators, legal scholars and other users of the text. After discussion, the Working Group decided that the section concerning the history of the draft Model Law should be maintained in its current form.

147. A similar debate took place regarding the section of the draft guide dealing with the description of PKI issues. The view was expressed that the technology described in the draft guide might become rapidly obsolete. Placing too much emphasis on the technological background against which the draft Model Law had been prepared, might adversely affect the ability of the instrument to stand the test of time. However, the widely prevailing view was that, while the draft Model Law had been prepared in technologically-neutral terms, precisely with a view to reinforcing its durability, it was important to provide its readers with a somewhat detailed view of

the technical environment that prevailed at the time when it was prepared. It was also felt that another reason for maintaining in the draft guide a comprehensive description of the technical environment of the draft Model Law was to make such information broadly available in those parts of the World where potential users of the draft Model Law and the draft guide might not be expected to be familiar with the technology and its state-of-the-art developments. After discussion, the Working Group decided that the various parts of the draft guide dealing with technology should be maintained in their current form. The possibility of introducing additional explanations might be considered by the Secretariat when revising the draft guide, with a view to making it abundantly clear that the draft Model Law was intended by its authors to offer sufficient flexibility to remain useful through some of the foreseeable technological changes.

B. Specific remarks

148. For lack of sufficient time, the Working Group did not engage in a detailed review of the various paragraphs of the draft guide. However, suggestions were made for certain changes, as reported below.

149. Regarding paragraph 32 of document A/CN.9/WG.IV/WP.86, it was generally felt that it would be misleading to suggest that, in the preparation of the draft Model Law, the Working Group had not received sufficient information as to the technical and legal implications of using "signature" devices relying on techniques other than public-key cryptography. It was recalled that numerous presentations had been made by experts regarding, for example, electronic signatures based on biometrics and other non-PKI-based technologies. After discussion, the Working Group decided that paragraph 32 should be deleted.

150. In paragraph 30 of document A/CN.9/WG.IV/WP.86, it was agreed that the words "other models are conceivable" should be replaced by "other models are already commonly used in the marketplace". In paragraphs 31 and 81 a sentence should be added along the following lines: "Other techniques involve the use of personal identification numbers (PINs), digitized signatures, and other methods, such as clicking an OK-box".

151. A suggestion was made for inclusion after paragraph 26 of a new paragraph as follows: "It should be noted that some countries consider that the legal issues related to the use of electronic signatures have already been solved by the UNCITRAL Model Law on Electronic Commerce, and do not plan on adopting further rules on electronic signatures until market practices in this new area are better established". While the suggested text was found generally acceptable as a statement of the legislative policy followed in some States, the Working Group generally agreed that appropriate wording should be added to the suggested new paragraph to describe the benefits expected from enactment of the draft Model Law and encourage States to adopt it alongside the UNCITRAL Model Law on Electronic Commerce.

152. With respect to paragraph 22 of document A/CN.9/WG.IV/WP.86/Add.1, the view was expressed that the draft guide should reflect the practices that involved the use of "split keys", i.e. situations where a single key was operated by two or more persons whose joint action was necessary to make the signature creation data operational. It was generally agreed that a sentence should be added to paragraph 22 along the following lines: "Where a single key is operated by more than one person in the context of a "split-key" or other "shared-secret" scheme, reference to "the signatory" means a reference to those persons jointly".

Notes

1 Official Records of the General Assembly, Fifty-first Session, Supplement No. 17 (A/51/17), paras. 223-224.

2 Ibid., Fifty-second Session, Supplement No. 17 (A/52/17), paras. 249-251.

3 Ibid., Fifty-third Session, Supplement No. 17 (A/53/17), paras. 207-211.

4 Ibid., Fifty-fourth Session, Supplement No. 17 (A/54/17), paras. 308-314.

5 Ibid., Fifty-fifth Session, Supplement No. 17 (A/55/17), paras. 380-389.

Annex

Draft UNCITRAL Model Law on Electronic Signatures

(as approved by the UNCITRAL Working Group on Electronic Commerce at its thirty-seventh session, held at Vienna from 18 to 29 September 2000)

Article 1. Sphere of application

This Law applies where electronic signatures are used in the context* of commercial** activities. It does not override any rule of law intended for the protection of consumers.

*The Commission suggests the following text for States that might wish to extend the applicability of this Law:

"This Law applies where electronic signatures are used, except in the following situations: [...]."

**The term "commercial" should be given a wide interpretation so as to cover matters arising from all relationships of a commercial nature, whether contractual or not. Relationships of a commercial nature include, but are not limited to, the following transactions: any trade transaction for the supply or exchange of goods or services; distribution agreement; commercial representation or agency; factoring; leasing; construction of works; consulting; engineering; licensing; investment; financing; banking; insurance; exploitation agreement or concession; joint venture and other forms of industrial or business cooperation; carriage of goods or passengers by air, sea, rail or road.

Article 2. Definitions

For the purposes of this Law:

(a) "Electronic signature" means data in electronic form in, affixed to, or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and indicate the signatory's approval of the information contained in the data message;

(b) "Certificate" means a data message or other record confirming the link between a signatory and signature creation data;

(c) "Data message" means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy;

(d) "Signatory" means a person that holds signature creation data and acts either on its own behalf or on behalf of the person it represents;

(e) "Certification service provider" means a person that issues certificates and may provide other services related to electronic signatures;

(f) "Relying party" means a person that may act on the basis of a certificate or an electronic signature.

Article 3. Equal treatment of signature technologies

Nothing in this Law, except article 5, shall be applied so as to exclude, restrict or deprive of legal effect any method of creating an electronic signature that satisfies the requirements referred to in article 6 (1) or otherwise meets the requirements of applicable law.

Article 4. Interpretation

(1) In the interpretation of this Law, regard is to be had to its international origin and to the need to promote uniformity in its application and the observance of good faith.

(2) Questions concerning matters governed by this Law which are not expressly settled in it are to be settled in conformity with the general principles on which this Law is based.

Article 5. Variation by agreement

The provisions of this Law may be derogated from or their effect may be varied by agreement, unless that agreement would not be valid or effective under applicable law.

Article 6. Compliance with a requirement for a signature

(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used which is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

(2) Paragraph (1) applies whether the requirement referred to therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

(3) An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph (1) if:

(a) the signature creation data are, within the context in which they are used, linked to the signatory and to no other person;

(b) the signature creation data were, at the time of signing, under the control of the signatory and of no other person;

(c) any alteration to the electronic signature, made after the time of signing, is detectable; and

(d) where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.

(4) Paragraph (3) does not limit the ability of any person:

(a) to establish in any other way, for the purpose of satisfying the requirement referred to in paragraph (1), the reliability of an electronic signature; or

(b) to adduce evidence of the non-reliability of an electronic signature.

(5) The provisions of this article do not apply to the following: [...]

Article 7. Satisfaction of article 6

(1) *[Any person, organ or authority, whether public or private, specified by the enacting State as competent]* may determine which electronic signatures satisfy the provisions of article 6.

(2) Any determination made under paragraph (1) shall be consistent with recognized international standards.

(3) Nothing in this article affects the operation of the rules of private international law.

Article 8. Conduct of the signatory

(1) Where signature creation data can be used to create a signature that has legal effect, each signatory shall:

(a) exercise reasonable care to avoid unauthorized use of its signature creation data;

(b) without undue delay, notify any person that may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature if:

(i) the signatory knows that the signature creation data have been compromised; or
(ii) the circumstances known to the signatory give rise to a substantial risk that the signature creation data may have been compromised;

(c) where a certificate is used to support the electronic signature, exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signatory which are relevant to the certificate throughout its life-cycle, or which are to be included in the certificate.

(2) A signatory shall be liable for its failure to satisfy the requirements of paragraph (1).

Article 9. Conduct of the certification service provider

(1) Where a certification service provider provides services to support an electronic signature that may be used for legal effect as a signature, that certification service provider shall:

(a) act in accordance with representations made by it with respect to its policies and practices;

(b) exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life-cycle, or which are included in the certificate;

(c) provide reasonably accessible means which enable a relying party to

ascertain from the certificate:

(i) the identity of the certification service provider;
(ii) that the signatory that is identified in the certificate had control of the signature creation data at the time when the certificate was issued;
(iii) that signature creation data were valid at or before the time when the certificate was issued;

(d) provide reasonably accessible means which enable a relying party to ascertain, where relevant, from the certificate or otherwise:

(i) the method used to identify the signatory;
(ii) any limitation on the purpose or value for which the signature creation data or the certificate may be used;
(iii) that the signature creation data are valid and have not been compromised;
(iv) any limitation on the scope or extent of liability stipulated by the certification service provider;
(v) whether means exist for the signatory to give notice pursuant to article 8 (1) (b);
(vi) whether a timely revocation service is offered;

(e) where services under paragraph (d) (v) are offered, provide a means for a signatory to give notice pursuant to article 8 (1) (b) and, where services under paragraph d (vi) are offered, ensure the availability of a timely revocation service;

(f) utilize trustworthy systems, procedures and human resources in performing its services.

(2) A certification service provider shall be liable for its failure to satisfy the requirements of paragraph (1).

Article 10. Trustworthiness

For the purposes of article (9) (1) (f), in determining whether, or to what extent, any systems, procedures and human resources utilized by a certification service provider are trustworthy, regard may be had to the following factors:

(a) financial and human resources, including existence of assets;

(b) quality of hardware and software systems;

(c) procedures for processing of certificates and applications for certificates and retention of records;

(d) availability of information to signatories identified in certificates and to potential relying parties;

(e) regularity and extent of audit by an independent body;

(f) the existence of a declaration by the State, an accreditation body or the certification service provider regarding compliance with or existence of the foregoing; or

(g) any other relevant factor.

Article 11. Conduct of the relying party

A relying party shall bear the legal consequences of its failure to:

(a) take reasonable steps to verify the reliability of an electronic signature; or

(b) where an electronic signature is supported by a certificate, take reasonable steps to:

(i) verify the validity, suspension or revocation of the certificate; and
(ii) observe any limitation with respect to the certificate.

Article 12. Recognition of foreign certificates and electronic signatures

(1) In determining whether, or to what extent, a certificate or an electronic signature is legally effective, no regard shall be had to:

(a) the geographic location where the certificate is issued or the electronic signature created or used; or

(b) the geographic location of the place of business of the issuer or signatory.

(2) A certificate issued outside *[the enacting State]* shall have the same legal effect in *[the enacting State]* as a certificate issued in *[the enacting State]* if it offers a substantially equivalent level of reliability.

(3) An electronic signature created or used outside *[the enacting State]* shall have the same legal effect in *[the enacting State]* as an electronic signature created or used in *[the enacting State]* if it offers a substantially equivalent level of reliability.

(4) In determining whether a certificate or an electronic signature offers a substantially equivalent level of reliability for the purposes of paragraphs (2) or (3), regard shall be had to recognized international standards and to any other relevant factors.

(5) Where, notwithstanding paragraphs (2), (3) and (4), parties agree, as between themselves, to the use of certain types of electronic signatures or certificates, that agreement shall be recognized as sufficient for the purposes of cross-border recognition, unless that agreement would not be valid or effective under applicable law.